

Notice of Allowability

Application No.

09/854,492

Applicant(s)

WOLFF ET AL.

Examiner

Michael Pyzocha

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 11/13/06.
2. ☒ The allowed claim(s) is/are 1-6, 8-17, 19-28, 30-39, 41-50, 52-61 and 63-74.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Art Unit: 2137

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin Zilka on 03/01/2007.

The application has been amended as follows:

Art Unit: 2137

1. (currently amended) A computer program product comprising a computer program operable to control a reporting computer to report occurrence of an event to a receiving computer, said computer program comprising:

report generating logic operable to generate report data identifying said reporting computer and said event;

data-retrieving logic operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

report sending logic operable to send said report data from said reporting computer to said receiving computer during said fetch of said requested data;

wherein said data retrieving logic and said report sending logic use an internet URL to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving ~~computer.~~ computer;

wherein said report data includes:

an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event and

a checksum of a file that triggered said event.

Art Unit: 2137

2. (original) A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing an unwanted computer program.

3. (original) A computer program product as claimed in claim 2, wherein said unwanted computer program is a computer virus.

4. (original) A computer program product as claimed in claim 1, wherein said requested data is a description of said event.

5. (original) A computer program product as claimed in claim 1, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

6. (original) A computer prepare product as claimed in claim 1, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

7. (cancelled)

8. (previously presented) A computer program product as claimed in claim 1, wherein said reporting computer collates report data specifying one or more events that is sent together

Art Unit: 2137

from said reporting computer to said receiving computer during said fetch of said requested data.

9. (original) A computer program product as claimed in claim 1, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

10. (original) A computer program product as claimed in claim 1, wherein said reporting computer and said receiving computer communicate via an internet link.

11. (currently amended) A computer program product as claimed in claim 1, wherein said report data further includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

Art Unit: 2137

an identifier of an event type detected by said reporting
~~computer;~~ computer; and

an action taken by said reporting computer upon detection
of said event. ~~event;~~ and

~~a checksum of a file that triggered said event.~~

12. (currently amended) A computer program product
comprising a computer program operable to control a receiving
computer to receive a report of occurrence of an event from a
reporting computer, said computer program comprising:

data request receiving logic operable to receive a request
for requested data from said reporting computer;

data providing logic operable to provide said requested
data to said reporting computer;

and

report receiving logic operable to receive report data
identifying said reporting computer and said event from said
reporting computer during providing of said requested data to
said reporting computer;

wherein said data retrieving logic and said report sending
logic use an internet URL to specify said requested data to said
receiving computer, said internet URL specifying said requested
data also containing said report data to be sent to said
receiving ~~computer.~~ computer;

Art Unit: 2137

wherein said report data includes:

an identifier of a set of event detecting data used by
a computer program used by said reporting computer to
detect said event and

a checksum of a file that triggered said event.

13. (original) A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing an unwanted computer program,

14. (original) A computer program product as claimed in claim 13, wherein said unwanted computer program is a computer virus.

15. (original) A computer program product as claimed in claim 12, wherein said requested data is a description of said event.

16. (original) A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

17. (original) A computer program product as claimed in claim 12, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

Art Unit: 2137

18. (cancelled)

19. (previously presented) A computer program product as claimed in claim 12, wherein said report data specifies one or more events and is sent together from said reporting computer to said receiving computer during providing of said requested data.

20. (original) A computer program product as claimed in claim 12, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

21. (original) A computer program product as claimed in claim 12, wherein said reporting computer and said receiving computer communicate via an internet link.

22. (currently amended) A computer program product as claimed in claim 12, wherein said report data further includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

Art Unit: 2137

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

an identifier of an event type detected by said reporting ~~computer;~~ computer; and

an action taken by said reporting computer upon detection of said event. ~~event;~~ and

~~a checksum of a file that triggered said event.~~

23. (currently amended) A method of controlling a reporting computer to report occurrence of an event to a receiving computer, said method comprising the steps of:

generating report data identifying said reporting computer and said event;

fetching requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

sending said report data from said reporting computer to said receiving computer during fetching of said requested data;

wherein an interact URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving ~~computer.~~ computer;

Art Unit: 2137

wherein said report data includes:

an identifier of a set of event detecting data used by
a computer program used by said reporting computer to
detect said event and

a checksum of a file that triggered said event.

24. (original) A method as claimed in claim 23, wherein said event is detection of a computer file containing an unwanted computer program.

25. (original) A method as claimed in claim 24, wherein said unwanted computer program is a computer virus.

26. (original) A method as claimed in claim 23, wherein said requested data is a description of said event.

27. (original) A method as claimed in claim 23, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

28. (original) A method as claimed in claim 23, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

29. (cancelled)

30. (previously presented) A method as claimed in claim 23, wherein said reporting computer collates report

Art Unit: 2137

data specifying one or more events that is sent together from said reporting computer to said receiving computer during fetching of said requested data.

31. (original) A method as claimed in claim 23, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

32. (original) A method as claimed in claim 23, wherein said reporting computer and said receiving computer communicate via an internet link.

33. (currently amended) A method as claimed in claim 23, wherein said report data further includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

Art Unit: 2137

an identifier of an event type detected by said reporting
~~computer;~~ computer; and

an action taken by said reporting computer upon detection
of said event. ~~event;~~ and

~~a checksum of a file that triggered said event.~~

34. (currently amended) A method of controlling a receiving
computer to receive a report of occurrence of an event from a
reporting computer, said method comprising the steps of:

receiving a request tot requested data from said reporting
computer;

providing said requested data to said reporting computer;
and

receiving report data identifying said reporting computer
and said event from said reporting computer during providing of
said requested data to said reporting computer;

wherein an internet URL is used to specify said requested
data to said receiving computer, said interact URL specifying
said requested data also containing said report data to be sent
to said receiving ~~computer.~~ computer;

wherein said report data includes:

an identifier of a set of event detecting data used by
a computer program used by said reporting computer to
detect said event and

Art Unit: 2137

a checksum of a file that triggered said event.

35. (original) A method as claimed in claim 34, wherein said event is detection of a computer file containing an unwanted computer program.

36. (original) A method as claimed in claim 35, wherein said unwanted computer program is a computer virus.

37. (original) A method as claimed in claim 34, wherein said requested data is a description of said event.

38. (original) A method as claimed in claim 34, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

39. (original) A method as claimed in claim 34, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

40. (cancelled)

41. (previously presented) A method as claimed in claim 34, wherein said report data specifies one or more events and is sent together from said reporting computer to said receiving computer during providing of said requested data.

Art Unit: 2137

42. (original) A method as claimed in claim 34, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

43. (original) A method as claimed in claim 34, wherein said reporting computer and said receiving computer communicate via an internet link.

44. (currently amended) A method as claimed in claim 34, wherein said report data further includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

an identifier of an event type detected by said reporting ~~computer;~~ computer; and

an action taken by said reporting computer upon detection of said event. ~~event; and~~

Art Unit: 2137

~~a checksum of a file that triggered said event.~~

45. (previously presented) A reporting computer operable to report occurrence of an event to a receiving computer, said reporting computer comprising:

a report generator operable to generate report data identifying said reporting computer and said event;

a data retriever operable to fetch requested data from said receiving computer to said reporting computer upon a request of said reporting computer; and

a report sender operable to send said report data from said reporting computer to said receiving computer during said fetch of said requested data;

wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving ~~computer.~~ computer;

wherein said report data includes:

an identifier of a set of event detecting data used by
a computer program used by said reporting computer to
detect said event and

a checksum of a file that triggered said event.

Art Unit: 2137

46. (original) A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing an unwanted computer program.

47. (original) A reporting computer as claimed in claim 46, wherein said unwanted computer program is a computer virus.

48. (original) A reporting computer as claimed in claim 45, wherein said requested data is a description of said event,

49. (original) A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

50. (original) A reporting computer as claimed in claim 45, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

51. (cancelled)

52. (previously presented) A reporting computer as claimed in claim 45, wherein said reporting computer generates report data specifying one or more events that is sent together from said reporting computer to said receiving computer during said fetch of said requested data.

Art Unit: 2137

53. (original) A reporting computer as claimed in claim 45, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

54. (original) A reporting computer as claimed in claim 45, wherein said reporting computer and said receiving computer communicate via an interact link.

55. (currently amended) A reporting computer as claimed in claim 45, wherein said report data further includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

an identifier of an event type detected by said reporting ~~computer;~~ computer; and

Art Unit: 2137

an action taken by said reporting computer upon detection of said event. ~~event;~~ and

~~a checksum of a file that triggered said event.~~

56. (currently amended) A receiving computer operable to receive a report of occurrence of an event from a reporting computer, said receiving computer comprising:

a data request receiver operable to receive a request for requested data from said reporting computer;

a data provider operable to provide said requested data to said reporting computer; and

a report receiver operable to receive report data identifying said reporting computer and said event from said reporting computer during providing of said requested data to said reporting computer;

wherein an internet URL is used to specify said requested data to said receiving computer, said internet URL specifying said requested data also containing said report data to be sent to said receiving ~~computer~~. computer;

wherein said report data includes:

an identifier of a set of event detecting data used by
a computer program used by said reporting computer to
detect said event and

a checksum of a file that triggered said event.

Art Unit: 2137

57. (original) A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing an unwanted computer program.

58. (original) A receiving computer as claimed in claim 57, wherein said unwanted computer program is a computer virus.

59. (original) A receiving computer as claimed in claim 56, wherein said requested data is a description of said event.

60. (original) A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing a computer virus and said requested data is a description of said computer virus.

61. (original) A receiving computer as claimed in claim 56, wherein said event is detection of a computer file containing a computer virus and said requested data is an updated set of computer virus detecting data for use in detecting computer viruses.

62. (cancelled)

63. (previously presented) A receiving computer as claimed in claim 56, wherein said report data specifies one or more events and is sent together from said reporting computer to said receiving computer during providing of said requested data.

Art Unit: 2137

64. (original) A receiving computer as claimed in claim 56, wherein said report data is encrypted by said reporting computer and decrypted by said receiving computer.

65. (original) A receiving computer as claimed in claim 56, wherein said reporting computer and said receiving computer communicate via an interact link.

66. (original) A receiving computer as claimed in claim 56, wherein said report data further includes one or more of:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

an identifier of an event type detected by said reporting ~~computer;~~ computer; and

an action taken by said reporting computer upon detection of said event. ~~event; and~~

Art Unit: 2137

~~a checksum of a file that triggered said event.~~

67. (previously presented) A computer program product as claimed in claim 1, wherein said report data further includes:

a MAC address identifying a network card of said reporting computer;

a date of said event;

a time of said event;

an identifier of a computer program used by said reporting computer to detect said event;

an identifier of a version of a computer program used by said reporting computer to detect said event;

~~an identifier of a set of event detecting data used by a computer program used by said reporting computer to detect said event;~~

an identifier of an event type detected by said reporting ~~computer;~~ computer; and

an action taken by said reporting computer upon detection of said event. ~~event;~~ and

~~a checksum of a file that triggered said event.~~

68. (previously presented) A computer program product as claimed in claim 1, wherein said interact URL includes a name of a script running on said receiving computer and encrypted report data.

Art Unit: 2137

69. (previously presented) A computer program product as claimed in claim 68, wherein said script decrypts said encrypted report data.

70. (previously presented) A computer program product as claimed in claim 1, wherein said report data includes an identifier of a driver triggered during said event.

71. (previously presented) A computer program claimed in claim 70, wherein said identifier of said driver is mapped to an identity of a virus that triggered mid event.

72. (previously presented) A computer program product as claimed in claim 1, wherein said UR.L is not displayed on said reporting computer.

73. (previously presented) A computer program product as claimed in claim 72, wherein said URL is in the form of a hypertext link that is associated with a description of said event.

74. (previously presented) A computer program product as claimed in claim 73, wherein selection of said hypertext link results in a URL request being passed to said receiving computer.

Art Unit: 2137

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance: The prior art teaches sending report data via unique URLs to send and receive data, but fails to explicitly disclose sending the identifier of the set of event detecting data used and the checksum of a file in the URL.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Symantec, Computer Associates, Trend Micro, and McAfee each teach methods of sending and receiving report data via unique URLs.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael. Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP